TERMS AND RULES OF THE POSTI BUG BOUNTY PROGRAM

The purpose of this program is to reward people who bring to our attention critical security vulnerabilities related to Posti services (See more at section "SCOPE OF THE PROGRAM"). Hackrfi Ltd acts as the coordinator of this program.

The rules, terms and conditions detailed in this document are applied to the Posti Bug Bounty Program. To avoid any confusion and misunderstanding, we recommend you read this document carefully before taking part in the program.

ABOUT THE PROGRAM

To encourage the security community to find security vulnerabilities and to disclose them responsibly, we offer bounties for accepted security vulnerabilities which are reported to us via the service at Hackrfi. A security vulnerability is a problem which causes the target system to lose confidentiality, integrity or availability.

You must follow the rules detailed in this document to prevent unforeseen security problems to the clients of Posti, their data or the business of Posti itself.

SCOPE OF THE PROGRAM

The full scope of URL's and applications of this program is maintained and updated in the Hackrfi portal (https://porkkana.hackr.fi).

What we are particularly interested in:

- All kinds of privacy issues, protection of client (consumer) data and information from unauthorized disclosure to data loss.
- Issues related to managing letters, invoices and parcels within Posti digital services
- Payment system security, payment method handling and/or loss or abuse of payment methods.
- Methods of blocking, slowing down or causing other availability issues to the systems.

Findings are assessed based on business impact. Findings which cause very small monetary losses or have minor business impact may not be eligible for bounties.

PRINCIPLES OF THE PROGRAM

We appreciate your co-operation in enhancing the security of Posti and its customers. The following key principles apply to this program:

- **Respect the law**: Respect the laws of your country and Finland as applicable.
- **Independence**: Persons taking part in the Bug Bounty program may not be involved in the development of applications in the program scope
- **Do it on your own**: The vulnerability research should be conducted from systems you own and manage yourself.
- **Limit collateral damages**: Design your research so that it uses a minimal viable attack to demonstrate a vulnerability. That is, the attack (for example the network load) or its effects (for example a database dump) should not be larger than necessary to verify the existence of a vulnerability.
- **Allow business to run**: Your vulnerability research must not significantly impact the availability of the services in scope.
- **Non-disclosure**: If you uncover a vulnerability that reveals information that would not be available to you without the vulnerability, you must not disclose, reveal or otherwise communicate this information to third parties.

If you have any questions or need clarification, please contact the bounty program coordinator Hackrfi Ltd via the contact forms in www.hackr.fi before taking part in the program.

We respect the time you invest in this program and we wish you correspondingly respect the times for reply and response we have defined for this program.

METHODS AND ACTIONS NOT ALLOWED

If we find out some of the following methods or actions have been used during the security research, it will cause the researcher to be disqualified from the program and potentially to criminal charges. We will not allow any methods or actions which will cause disruption to the availability of the services or have negative impact to the clients or customers of Posti, including but not limited to the following.

- Code injections to the backend systems (for example SQL-injection) where the data in the backend is changed or deleted or read in unnecessary quantities. Code injections themselves are allowed, the limitation is the to the functionality and scope of the research and Proof of Concept code. For example, you can read some data to

demonstrate the vulnerability but do not dump all the data, nor delete or change any data.
- Denial of Service, “DoS”. This also applies to any tools or scanners that may cause denial of service type of load.
- Social engineering and man-in-the-middle attacks.
- Actions and methods that cause, or will probably cause, disruption to the business.
- Any actions that threaten the security of an individual persons.

HOW TO REPORT A VULNERABILITY

A security vulnerability shall be reported through a submission form dedicated to this program. The submission form is located in the Hackrfi reporting portal.

When submitting a report, one should ensure the following:

- The reporter should share all the possible information and details regarding the finding to help us replicate and verify the finding. We cannot award a bounty if we can’t replicate the issue. Do not leave out any information to use later for similar new reports or findings.
- We aim to respond to the reporter within five (5) work days from the day we receive a submitted report to inform how the case is progressing.
- We aim to confirm the reported finding within fourteen (14) work days from the day we’ve received the report. Please notice that this is an indicative target and the confirmation process might take longer. It is important to notice that time needed for confirmation depends on how comprehensive the report is and how complicated it is to reproduce the reported vulnerability.
- Research and testing shall not pose a threat or danger to other users of the service – if needed please ask for permission before testing.
- If a participant has a suspicion that future steps or procedures in one’s research might cause disruption in the service, an incomplete report can be submitted with a request for a permission to continue research.

Findings and bugs that are not security or privacy related and any customer service contacts that are submitted through the submission form dedicated to reporting will be ignored. If you have such matters, we kindly ask you to contact us straight through our contact form on the Hackrfi home page or in the Hackrfi reporting portal.

CONTENTS OF THE REPORT

We need to be able to verify the vulnerability in the report. If we cannot verify the issue by reproducing it, we cannot award a bounty. If the vulnerability is related to a web browser, we

need to be able to replicate it with a relatively modern browser (HTML5 compatible).

There are classes of reports that may not be accepted to be eligible for a bounty in this program.

- Report by an automated scanner, which in general are very speculative and tentative.
- Configuration issues with email servers (SPF, DMARC, ...)
- SSL/TLS configuration best practices or the lack of them (unless there is a clear and demonstrable vulnerability).
- Issues related to SSL/TLS configuration which are found by SSLabs scanner or similar.
- Best practices or the lack of them related to HTTP security headers.
- Forms with a theoretical CSRF vulnerability. CSRF vulnerabilities with a clear impact and a working PoC may be accepted. Logout CSRF's are always out of scope.
- Reports related to password strength or quality.
- Information disclosure of version numbers or similar, which are not related to a definite exploitable vulnerability.
- Reports related to cookies and their configuration.
- Issues in error page configuration.
- Any observations from issues, vulnerabilities and problems which are not under the control of Posti.

OTHER THINGS TO NOTE

When the reporter sends a vulnerability report, they will agree not to publish or disclose the vulnerability. The bounty will not be paid if a third party receives information on the reported vulnerability. The reporter will also agree not to use the vulnerability for personal gain.

If several people report the same vulnerability, only the first reporter will receive the bounty by default. Subsequent reporters will be informed that the vulnerability is a duplicate and has already been reported.

BOUNTIES

The largest bounty is 10.000€ and the smallest is 100€. Bounties are paid according to the Finnish law as compensation for work ("työkorvaus"), not as salary, and Hackrfi Ltd will be paying the bounties on behalf of Posti.

The size of the bounty awarded is determined by Posti. The bounties are determined based on the risk and impact level of the vulnerability. The reports are evaluated based on business impact. If the vulnerability reported does not create a risk or is not a security issue, we reserve the right to not award a bounty.

We aim to be open in determining the bounty amount by disclosing the reasoning behind the bounty to the reporter. If the vulnerability is in a publicly available and widely used library, we may award a bounty which is smaller than usual.

If you report several vulnerabilities which are triggered by the same root cause vulnerability, or the vulnerability is a smaller aspect of a bigger vulnerability, these reports can be combined when determining the bounty.

Due to regulations, we interact with the original reporter only when discussing the reported vulnerabilities.

ADDITIONAL LEGAL STATEMENTS

Posti and Hackrfi Ltd are reserving the right to discontinue this bug bounty program and change its terms at any time and without prior notification. All decisions regarding bounties and rewards are final. The rules of this bug bounty program or any communication related to this do not provide or imply any obligations of any kind from Hackrfi Ltd.

When submitting a security vulnerability to Hackrfi Oy, you will grant to Hackrfi Oy and Posti an eternal, worldwide, royalty-free, irrevocable, non-exclusive license and right to use, modify and integrate the information contained in the report to the services, products and test systems of Hackrfi Oy or Posti. Neither Hackrfi Ltd nor Posti have any obligations to the reporter for this bug bounty program.